18

Internetworking Objects with RFID

Rune Hylsberg Jacobsen, Qi Zhang, and Thomas Skjødebjerg Toftegaard
Aarhus School of Engineering, Aarhus University
Denmark

1. Introduction

The Internet of Things refers to the networked interconnection of everyday objects. Everyday objects, such as cars, coffee cups, refrigerators, bathtubs, and more advanced, loosely coupled, computer resources and information services will be in interaction range of each others and will communicate with one another. The Internet of Things has the potential to be used by billions of independent devices co-operating in large or small combinations, and in shared or separated federations. It is going to be based on information about objects in the physical world and their respective surroundings. This information will be provided by "the things", as they obtain and reveal information through RFID, wireless sensors and communication devices embedded in systems or worn by users. Through unique addressing schemes these things are able to be networked with each other on a global scale and to cooperate with neighbors and remote systems to reach common goals.

During the last few years an increasing number of conferences, workshops, research projects and coordinated actions on a global as well as European level shape the current understanding of the important topics of RFID and Future Internet including Internet of Things. Buckley (2006) summarized recent trends in Radio Frequency Identification (RFID) integration with Internet of Thing. The coordinated action CE RFID in Europe has published a Final report on RFID and its applications. In the report edited by Wiebking et al. (2008), a comprehensive summary of RFID and its applications are provided.

In a recent publication, Khoo (2010) reviews current RFID technology, its usage, and the necessary development required for RFID technology to enable the Internet of Things. Atzori et al. (2010) describes how the basic idea is to have the pervasive presence around us by using a variety of things or objects such as RFID tags, sensors, actuators, mobile phones etc.

The vision of an Internet of Things powered by next generation RFID has many potential advantages. It offers new industrial opportunities for the Information Communication Technology (ICT) market, and enable a breakthrough improvement in process efficiency and product/service quality in several application scenarios, such as environmental monitoring, e-health, intelligent transportation systems, military, and industrial plant monitoring. Moreover, it increases the usefulness of the Internet to the majority of citizens, who are interested in getting physical support to their daily needs.

RFID devices and systems are showing significant potentials in applications from manufacturing, security, logistics, airline baggage management to postal tracking. The technology enables an organization to re-engineer its business processes and to increase the efficiency that results in lower costs and higher effectiveness. Manufacturers and distributors deploy RFID to handle the logistical overload that results from the large increase in global sales from electronic commerce or to improve the efficiency of an enterprise supply chain.

While current deployment of RFID technology is focusing on use cases for object tracking and object monitoring, the integration with wireless sensor network (WSN) technology adds another dimension. The integration of RFID and WSN allows RFID tags and readers to form networks in order to implement complex functions where the communication of one tag and one reader is insufficient. The networks can be further enriched by the integration of sensors. One of these functions could be the range enhancement by distributing messages over multiple network nodes. Static network nodes could also locate each other as well as locate nodes moving within the network. By taking a holistic approach to RFID/WSN in the Internet of Things we move from connection of objects to the networking of objects.
This chapter discusses the RFID/WSN technology in a networking perspective. We outline the development needed to integrate RFID systems with the Internet of Thing and look at the evolution from today's connection of objects to the future networking of objects.

2. Internetworking scenarios

It can be observed that the Internet of Things should be considered as part of the overall Internet of the future, which is likely to be remarkably different from the Internet we use today. Fig. 1 illustrates this principle. A wide-spread interconnection of everyday objects to the Internet adds another "onion ring" to the communication infrastructure. As we move from

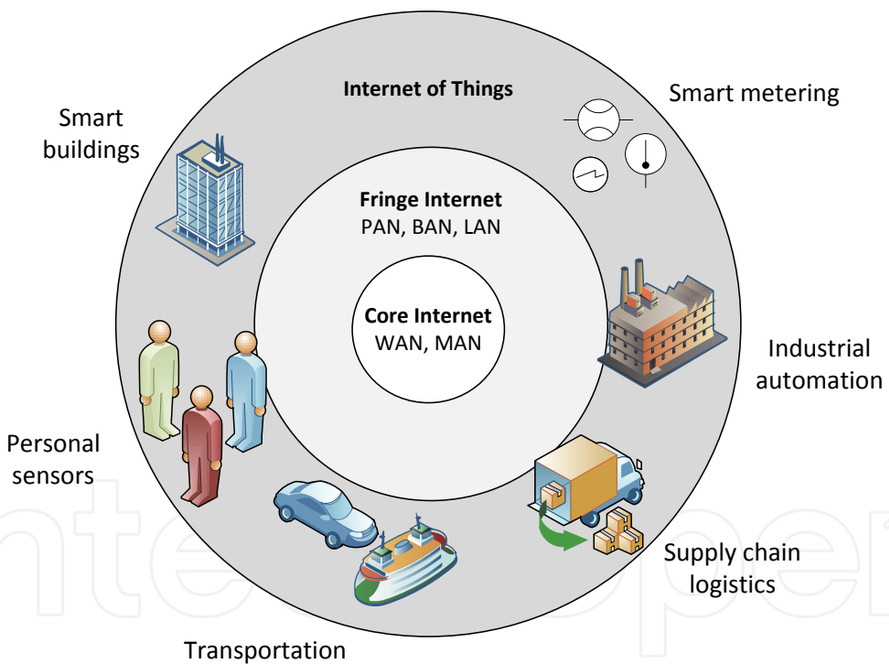


Fig. 1. Interconnecting objects to the Internet adds an outer "onion ring" to the communication infrastructure.

the core of the Internet with its high capacity routers to the outer network edges, i.e. the fringe Internet, where different local networks and access networks such as personal area networks (PAN), body area networks (BAN), local area networks (LAN) we gradually get closer to the physical objects in our surroundings.
The integration of RFID and WSN technology into the infrastructure adds new possible usages of RFID technology. Mitrokotsa & Douligeris (2010) describe how integrated RFID

sensor systems essentially allow two new categories of usage: First, integrated *RFID sensor-tag* will allow the tracking of sensor data of an object through-out its life-cycle. This might be very important for the transportation and storage of hazardous goods (e.g. chemicals, nuclear waste etc.), and medical samples that e.g. must stay within some temperature interval during transportation. Another possible use is to track the usage of a mechanical system known to be prone to failures due to fatigue built up over time such as a weapon system. These usage scenarios represent a further enhancement of the object tracking and object monitoring applications. When tags are brought into proximity of the reader an asynchronous data transfer can occur. Thus connecting the physical objects to the Internet. Second, integrated *RFID sensor-reader* systems will add the wireless networking dimension to the RFID system thereby introducing enhancements such as mobility support, naming and addressing, resiliency, end-to-end architectures, networking security etc. This allows portable readers to be connected to the Internet of Things whereby data can be readily accessed, processed and distributed over the Internet.

Fig. 2 and 3 illustrate two different network architectures for the integration of RFIDs and wireless sensor nodes. The integration of wireless sensing nodes with RFID tags allow devices

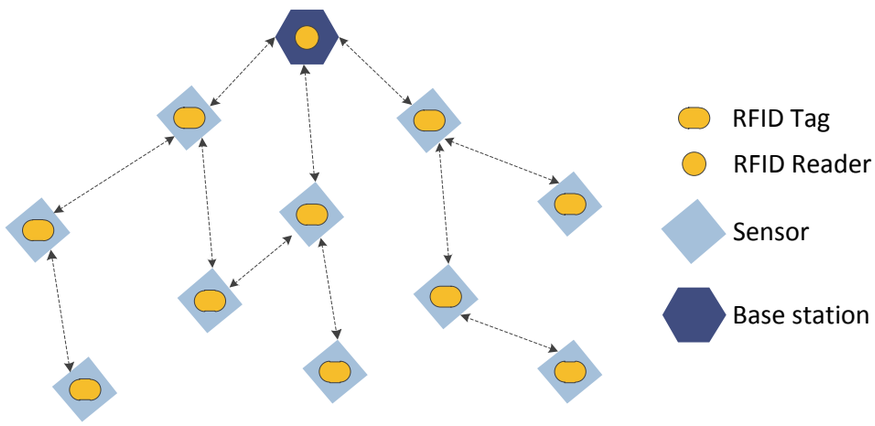


Fig. 2. RFID sensor-tag network architecture. (Adapted from Mitrokotsa & Douligeris (2010)).

to communicate with each other as well as with other wireless devices. The main feature of such integrated device is that the RFID sensor-tags can collect data related to the conditions around them and transmit and share these data with each other. The network of the integrated sensor-tags is able to communicate with a wider network, such as an enterprise network and/or the Internet, via base stations.

Another possible strategy of integrating RFID systems with WSNs is by integrating RFID readers with sensor nodes as shown in Fig. 3. Zhang & Wang (2006) labeled this integrated RFID sensor/reader node a "smart node" with the interpretation of "smart" meaning an autonomous physical/digital objects augmented with sensing, processing, and network capabilities. Smart nodes are able to relay information and to be configured as relay nodes or routers of a WSN. Likewise the RFID sensor-tags, smart nodes are able to communicate with each other by creating an ad hoc communication network. From an architecture point of view this integrated network, is similar to the hierarchical clustering-based two-tiered WSN.

RFID and WSN are key enablers to realize the Internet of Things scenario described above. On the other hand cost will be the key driver for the evolution. The main argument for bringing the WSN into the discussion is to offer connected mobility for relatively small and power/resource limited devices as an integral part of the Internet of Things. The necessity

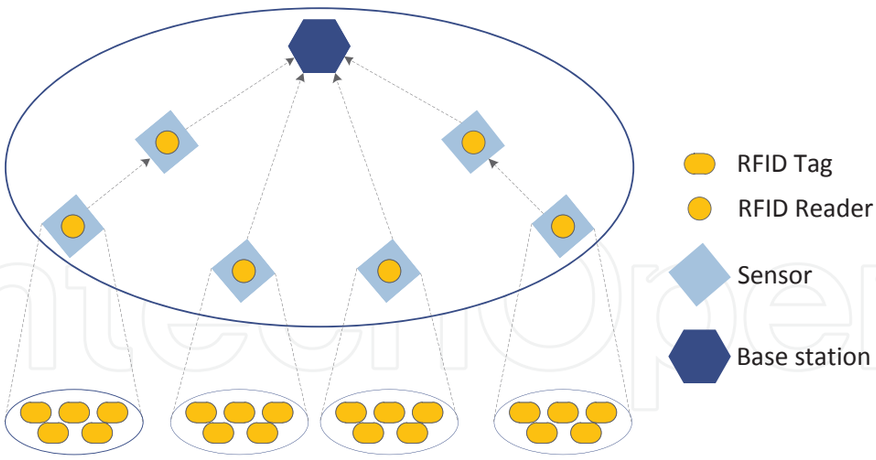


Fig. 3. RFID sensor-reader network architecture. (Adapted from Mitrokotsa & Douligeris (2010)).

for RFID is basically the same. However with a factor in increased volume of 1000 the constraints are even stronger. Especially the cost of the nodes becomes very critical. Given the potential ultra-low cost of RFID objects, as shown in e.g. Lakafosis et al. (2010) we can reach a completely new layer in the Internet of Things. Therefore the combination of the two will give us a technology with extended capabilities, scalability and of course portability while still being able to control the cost.

3. Technologies for identification, sensing and communication

In this section we introduce the essential technologies for identification, sensing and communication in the Internet of Things. We do not provide for an in-depth presentation of all relevant topics but merely focus on the technological aspects that are the most significant ones for an internetworking scenario. In the following we will address RFID system components, WSN technology as well as infrastructure aspects of the Internet of Things.

3.1 RFID systems

Several reviews and surveys of RFID technology have been published in the literature such as as the articles by Floerkemeier & Sarma (2008) and Krishna & Husalc (2007). Essentially, an RFID system is composed of a number of tags coupled with one or more readers that are connected to an ICT infrastructure. RFID tags (transponders) fall into two general categories, active and passive RFIDs, depending on their source of electrical power. RFID tags are typically of very small size and of very low cost. Passive tags harvest the energy required for transmitting their Identification (ID) from the query signal transmitted by a RFID reader (interrogator) in the proximity and their lifetime is not limited by the battery duration. An RFID reader communicates with one or more RFID tags via electromagnetic radio frequency fields. The radio frequency band used for RFID range from low frequency (LF), via high frequency (HF) up to ultra high frequencies (UHF). In fact, this signal generates a current into the tag antenna by induction. The current is utilized to supply the microchip which will transmit the tag ID. Usually, the antenna gain i.e. the power of the signal received by the reader divided by the power of the signal transmitted by the reader, of such systems is very low. Thanks to the highly directional antennas utilized by the RFID readers, tags ID can be correctly received within a radio range that can be on the order of few meters. At least the

reader reads tag ID. Furthermore, it may read auxiliary data from tags or write data to tags that support additional data memory (read only, read/write). The transmission of an RFID system is subjected to the same radio wave impairments as any other wireless communication systems.

Other RFID tags get power supplied by batteries. In this case we can distinguish between semi-passive and active RFID tags. For semi-passive RFID tags batteries are used to power the microchip while receiving the signal from the reader. Like in the passive RFID tags, the radio is powered with the energy harvested by the reader signal. In contrast, active RFID tags use the battery power for the transmission of the signals as well. Obviously the radio coverage is higher for active tags compared to the semi-passive and passive tags.

A typical RFID reader (interrogator) is comprised of a radio module, a central processing unit (CPU), a network interface, and general input/output pins. The CPU can be a low-end microcontroller or an advanced embedded microprocessor with significant computing resources. RFID readers do not require line-of-sight access to read the tag and the read range of RFID is larger than that of a bar code reader. Tags can store more data than bar codes and readers can communicate with multiple RFID tags simultaneously. Because of this capability, an RFID reader can capture the contents of an entire shipment as it is loaded into a warehouse or shipping container.

By using RFID it is possible to give each object, e.g. each product in a grocery store, its own unique object ID. There are several different standardized schemes for identifier encoding format. The unique object ID must have a global scope that is capable of identifying all objects uniquely and acts as a pointer to information stored about the object and the functionalities of the tag somewhere over the network. In general, the identification will be a number that contains information about the tags ID format, the organization issuing the tag, the class of the objects as well as serial number information.

3.2 Wireless sensor network technology

Several books and research papers exist on wireless sensor network (WSN) technology and applications such as e.g. Karl & Willig (2005). WSNs bring about key enabling technologies for the Internet of Things. Wireless sensor technologies allow objects to provide information about their environment and context, whereas smart technologies allow everyday objects to "think and interact".

WSNs have evolved from the idea that small wireless devices distributed over large geographical areas can be used to sense, collect, process, and distribute information from the physical environment. An essential building block of a wireless sensor is the microcontroller. The processor core can be 8-, 16- or 32-bit based but the CPU performance is not by itself that critical as a wireless sensor network is not expected to process large amount of data. WSN devices run with a low duty-cycle alternating between sleep and active mode. The active period of operation can be shorter with a more efficient CPU. The devices are unable to communicate during the sleep periods and in most scenarios WSN devices spend a large part of their time in a sleep mode to save energy and cannot communicate. This is absolutely anomalous for internetworking devices in today's Internet.

A WSN typically connects the physical environment to real-world applications, e.g., wireless sensors. Different wireless protocols have evolved for personal area networks and sensor networks as e.g. Z-wave and Zigbee with its IEEE 802.15.4 radios and several standards for wireless communication exist today. Until recently the perception has been that a full-fledged Internet Protocol (IP) communication stack was too large and complex to implement in small devices. However, a new and appealing wireless standard for interconnecting wireless sensor

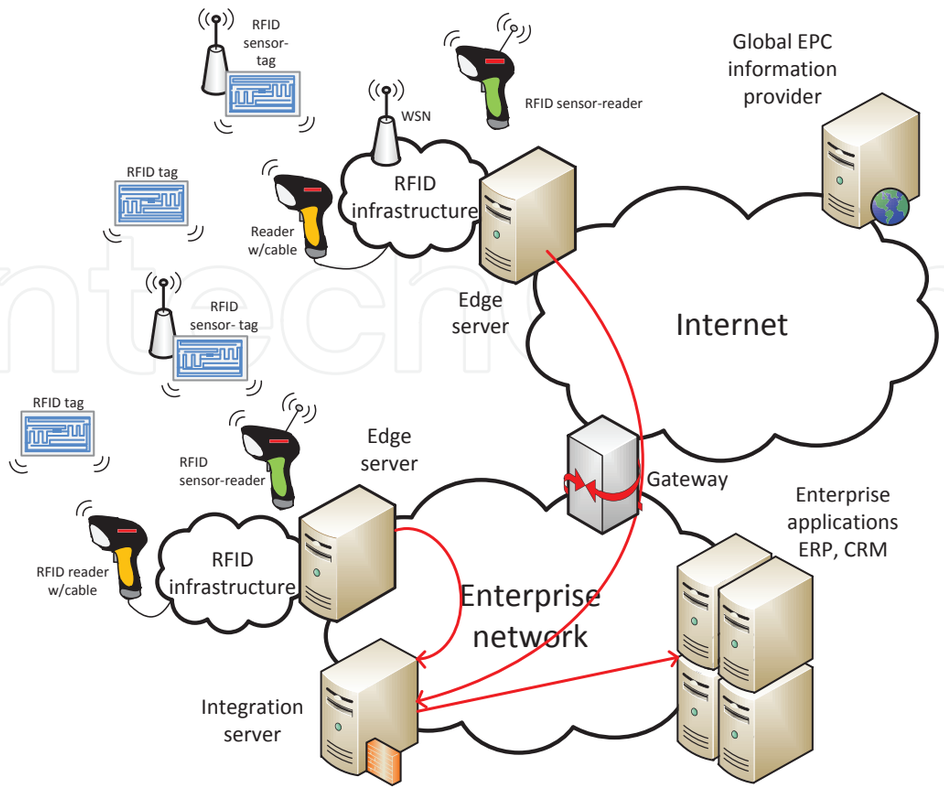


Fig. 4. RFID network scenario.

networks is the IEEE 802.15.4 standard. In this particular case it seems that through a wise Internet protocol adaptation, IEEE 802.15.4 devices can be incorporated into the Internet architecture. This allows us to rely on already adopted schemes for forwarding, routing, addressing etc.

WSNs can potentially consist of a very high number of sensing nodes communicating in a wireless multi-hop infrastructure. The number of nodes usually reports their sensing data to a small number (in most cases, only one) of special nodes called sinks.

3.3 Network reference model

From a networking perspective, an RFID system consists of several components that communicate. Typically an RFID system is built as an enterprise system that integrates RFID with enterprise legacy systems over a common ICT infrastructure. Together with existing enterprise systems, a RFID network system is built that may interact and communicate with other networks (e.g. business to business) as well. Fig. 4 shows a possible RFID scenario. Via a wired or wireless interface, the reader connects to an RFID edge server. This edge server adapts and co-ordinates the data transfer from a number of readers to enterprise resource planning systems (ERP), such as integration and/or control servers. RFID middleware running on the edge server helps to convert usually proprietary and incompatible interfaces between readers and enterprise systems.

Issues related to how to represent, store, interconnect, search, and organize information generated by the Internet of Things will become very challenging.

4. Integrations aspects of RFID/WSN in the Internet of things

Upon interconnecting objects to the Internet a number of central questions can be raised. How will the Internet architecture evolve when a large scale of limited devices represented by objects get globally connected? What is the essential protocols to use and what needs further development. How to provide application and service interoperability? And how can the security and privacy issues be handled? In this section we will discuss these aspects in more details.

4.1 Internet architecture evolution

The integration of RFID sensor networks in the Internet of Things adds further heterogeneity to the networks. We are working towards an evolved architectural model for the Internet of Things that supports a loosely coupled, decentralized system of smart objects. In contrast to simple RFID tags, smart objects carry chunks of application logic that let them interact more "intelligently" with human users.

The Internet of Things will include an incredibly high number of nodes, each of which will produce content that should be retrievable by any authorized user regardless of her/his position. To make a universal communication system there is a need for globally accepted methods of identifying how each object is attached to a network. This requires effective addressing schemes (and policies) by which objects can identify themselves, locate other objects and discover the communication path between them. Due to the rapid depletion of IPv4 addresses and its short address length (32-bit) it is clear that other addressing schemes than the IPv4 addressing scheme should be used. In this context IPv6 addressing has been proposed. IPv6 uses 128-bit addresses and therefore, it is possible to define on the order of 10^{38} addresses, which should be enough to identify any object which is worth to be addressed. Accordingly, we may think to assign an IPv6 address to all the things included in the network. Since RFID tags use 64 or 96-bit identifiers ways to associate RFID identifiers with network addresses can be inserted. One such method that has been proposed is the recent integration

	EPC^{TM}	**IPv6**
Scope	Global	Global
Namespace depth	3	3
Naming authority	EPCglobal	IANA
Identifying objects	All physical	All network interfaces
Length	64 or 96 bits	128 bits
Identifies through	Information pointers	Routing address
Identifier assignment	Permanet	Temporary

Table 1. Comparison between RFID EPC^{TM}identification and IPv6 addressing schemes.

of RFID tags into IPv6 networks. Table 1 compares the addressing schemes for RFID and IPv6 devices.

As an example for the 96-bit EPC^{TM}identification scheme the space for a company is 60 bits with 24-bit Object Class and 36-bit Serial Number. The standardization body EPCglobal assigns the General Manager Number. A single IPv6 subnet can map this entire space. With the integration, the RFID Object Class and Serial Number become the IPv6 Interface ID. This is illustrated in Fig. 5. So, each RFID tag can be addressable in the IPv6 network. The IPv6 prefix defines the scope of reach.

Another issue is the way in which addresses unknown to the requester are obtained. A name service is needed to map a reference to an address and a description of a specific object and

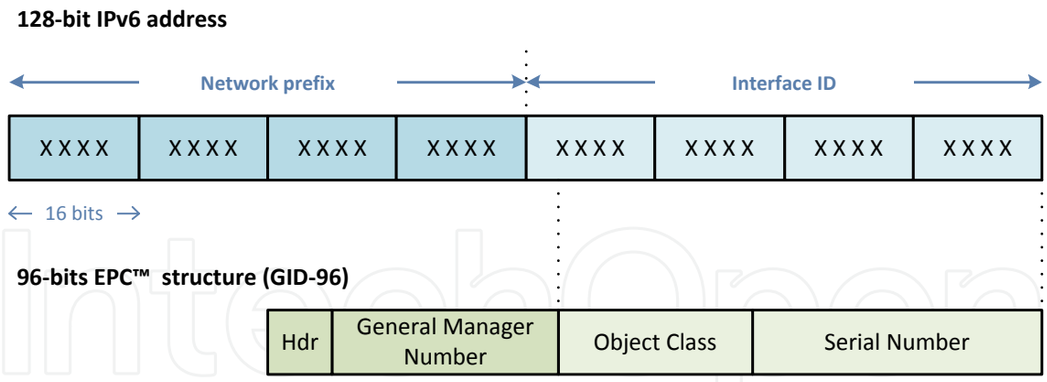


Fig. 5. IPv6-RFID address mapping with EPC^{TM}GID-96.

the related identifier, and vice versa. In today's Internet any host address is identified by querying appropriate domain name servers (DNS) that provide the IP address of a host from a certain input name. In the Internet of Things, communications are likely to occur between (or with) objects instead of hosts. Therefore, the concept of an Object Name Service (ONS) must be introduced, which associates a reference to a description of the specific object and the related RFID tag identifier.

Another promising usage for RFID in the Internet of Things is the potential support for mobility. Recently, Papapostolou & Chaouchi (2009) demonstrated the RFID-assisted IP mobility by using topology information provided by an RFID system to predict the next point of attachment of an RFID-enabled mobile node. There are several proposals for objects addressing but none for mobility support in the Internet of Things scenario, where scalability and adaptability to heterogeneous technologies represent crucial problems. The Internet of Things presents a further challenge that mobile objects may need to re-register their presence on different name servers as a consequence of moving.

4.2 Protocols

The OSI seven-layer model has conditioned a whole generation of telecommunications and information technology protocols. The basic concept of separating functionalities in layers according to clearly separated interfaces through protocols has proven to be powerful for large system designs. For resource limited devices or objects this approach is now showing its limitations. Protocols typically used in the Internet today need hundreds and more of kilobytes of program code to run but this is exceedingly too large for even device object with modest computing resources. Lighter protocols and lighter implementations that compress the explicit protocol layers into a single communications module are now required in the Internet of Things. The protocol header overhead introduced in each layer is a severe limitation to the effective data throughput of narrow-band wireless links. Therefore, existing data communication protocols may be inappropriate for the small objects of the Internet of Things.

New alternative cross-layer based protocols need to be re-engineered in order to cope with the changes that the connecting of objects bring. Stateful protocols as e.g. TCP cannot be used efficiently for the end-to-end transmission control in the Internet of Things. Furthermore, TCP requires excessive buffering to be implemented in objects and its connection setup and congestion control mechanisms may be useless. So far, no complete solutions have been proposed to solve this issue for the Internet of Things and therefore, research contributions

are required. There are several proposals for objects addressing but none for mobility support in the Internet of Things scenario.
Finally with the resource limited nodes and objects and the combination of RFID and WSN the Internet of Things is bound to deal with both an RFID protocol stack as well as a protocol stack for WSN e.g. IEEE 802.15.4 together with a higher layer internetworking protocol stack such as the 6LoWPAN stack.

4.3 Service-oriented architectures

Application and service interoperability is a key aspect for the success of the Internet of Things. In today's service architectures, a middleware layer that translates different data formats and protocols are typically implemented. User interfaces like web services offer necessary interaction and application control. However, according to Wiebking et al. (2008) conventional middleware is inappropriate for handling the range of devices needed for the pervasive internetworking of everyday objects.
Architectures proposed in the recent years for the Internet of Things often follow the service-oriented architecture (SOA) approach. The adoption of the SOA principle allows a decomposition of complex and monolithic systems into applications consisting of an ecosystem of simple and well-defined components that interplay. The use of common interfaces and standard protocols gives a horizontal view of a (potentially) globally distributed enterprise system. Advantages of the SOA approach are recognized in most studies on middleware solutions for Internet of Things. The development of business processes enabled by the SOA is the result of the process of designing workflows of coordinated services, which eventually are associated with objects actions. Furthermore, these processes can be directly linked to the business logic of the enterprise. This facilitates the interaction among the parts of an enterprise and allows for reducing the time necessary to adapt itself to the changes imposed by the market evolution.
An SOA approach does not impose a specific technology for the service implementation and hence allows for software and hardware reuse and can cope with a large degree of heterogeneity. Fig. 6 shows a simplified service architecture for an RFID enriched Internet of Things. The proposed solutions face essentially the same problems of abstracting the devices functionalities and communications capabilities, providing a common set of services and an

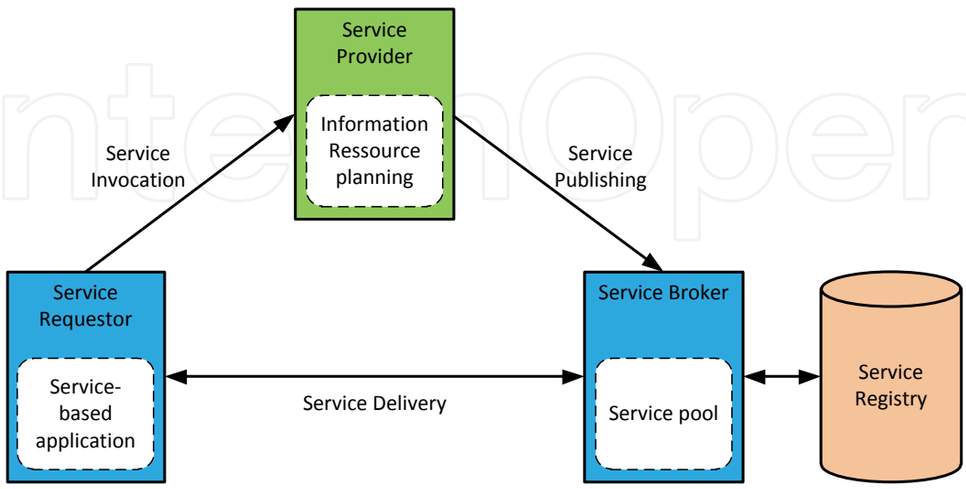


Fig. 6. Service architecture for RFID sensor-network system.

environment for service composition. These problems are further strengthened by the lack of resources available in the RFID/WSN devices. However, for most devices foreseen to be connected with objects in the Internet of Things, the SOA framework becomes impractical to be used because of its demands for computing resources.
Shelby (2010) describes the enabling for web services in contained devices such as WSN. In the described approach a RESTful service architecture based on light-weighted protocols and schemes are introduced to allow a transparent web service to become a reality. Functions that are not needed are omitted, redundant information compressed and service interoperability can be achieved.

4.4 Security and privacy

In general, good security depends on a holistic system-oriented view. Weis et al. (2004) reviews the security aspects related to RFID. From a networking point of view the security threats in an RFID empowered Internet of Things are much similar to that of wireless ad hoc and sensor networks. The wireless and distributed nature of the networks increases the spectrum of potential security threats. The threat model is further stressed by the resource constraints of the RFID/WSN devices. One major challenge in securing RFID tags is a shortage of computational resources within the tag. RFID sensor devices tend to be prone to failure, for example due to battery depletion. The lack of resources prevents intensive security approaches from being deployed. Standard cryptographic techniques require more resources than that is available in most low cost RFID devices. Therefore, manufacturers are looking at more light-weighted encryption schemes, but often with the trade-off in form of a weaker security. A viable security approach should adapt small code size, low power operation, low complexity, and small bandwidth across all nodes in the sensor network.
However, RFID also brings in new perspectives and challenges into the protection of systems, goods and other assets. End-to-end protection in the Internet of Things require confidentiality and integrity protection. This can be provided at the application, transport, network, and at the link layer. Daou et al. (2008) as well as Sharif & Potdar (2008) outline several of these aspects.
Authentication is difficult in the Internet of Things as it requires appropriate authentication infrastructures that will not be available in Internet of Things scenarios. Also the protection from man-in-the-middle attacks is a big challenge for the system design.
Data integrity is usually ensured by protecting data with passwords. However, the password lengths supported by Internet of Things technologies are in most cases too short to provide a strong level of protection.
The network used to share product data between trading partners i.e. EPCglobal Network, by design, is also susceptible to denial of service (DoS) attacks. Using similar mechanism with DNS in resolving EPC^{TM}data requests, the ONS root servers become vulnerable to DoS attacks. Any organization planning to implement RFID technology based on EPCglobal Network may discover that the EPCglobal Network infrastructure inherits security weaknesses similar to the weaknesses of DNS.
A second class of defense uses cryptography to prevent tag cloning. Some tags use a form of "rolling code" scheme, wherein the tag identifier information changes after each scan, thus reducing the usefulness of observed responses. More sophisticated devices engage in challenge-response authentication scheme where the tag interacts with the reader. In these protocols, secret tag information is never sent over the insecure communication channel between tag and reader in accordance with a well-defined protocol scheme. Rather, the reader issues a challenge to the tag, which responds with a result computed using a cryptographic

circuit keyed with some secret value. Such protocols may be based on symmetric or public key cryptography. From a networking point of view it is less evident if and how public key infrastructure can be adopted by RFID/WSN devices in the Internet of Things.
A primary security and privacy concern comes from the illicit tracking of RFID tags. Tags, which are readable, pose a risk to both personal location privacy and corporate/military security. Indeed, unseen by users, embedded RFID tags in our personal devices, clothes, and groceries can unknowingly be triggered to reply with their information. Hence, a lot of private information about a person can be collected without the person being aware. The control on the diffusion of all such information is impossible with current techniques. Potentially, this enables a surveillance mechanism that would pervade large parts of our lives. Privacy organizations have expressed concerns for the context of ongoing efforts to embed RFID tags in consumer products. Thus the essential question to address is how to provide user control over their own privacy for them to build trust in the systems. For RFID technology to be a successful part of the Internet of Things public entities need to be made aware that the pervasive networking concepts pose new challenges in terms of personal privacy.
The Internet of Things must be reliable and robust in the face of device malfunction, abnormal traffic loads and traffic patterns and malicious attack. It should safeguard policies regarding ownership of information and authority to access devices, giving due respect to people's rights of privacy.

5. The road ahead for Internetworking of objects

Regarding the future of RFID technologies, with a time horizon between medium-term (5-10 years) and long-term (10-20 years), it is obviously difficult to see where vision reaches beyond what is realistic. What seems clear today is that we are witnessing a paradigm shift from the "identification of objects at a distance" to the more challenging "communication between objects". This implies that besides the next generation of RFID technology there must be a scalable, efficient, reliable, secure and trustworthy infrastructure able to internetwork all involved objects. Technological issues relating to laws of physics must clearly be addressed.
In the European Union, as well as other places around the globe, Future Internet and Internet of Things has been a key strategic challenge for research and technological development. Wiebking et al. (2008) presents a focused roadmap for the Internet of Things that provides a forecast for the evolutions on medium-term and long-term. Among other things the roadmap addresses standardization efforts, technological trends, basic research, and interoperability aspects. Fig. 7 summarizes the road ahead for the evolution of Internet of Things based on a large scale of interconnected objects.

5.1 Standardization

RFID technology efforts towards standardization are focusing on principal areas such as RFID frequency spectrum usage and reader(s)-tags communication protocols, and data formats for tags and labels. The major standardization bodies dealing with RFID systems are EPCglobal, the European Telecommunications Standards Institute (ETSI), and the International Organization for Standardization (ISO). With respect to the Internet of Things, ETSI has started the Machine-to-Machine (M2M) Technical Committee to conduct standardization activities relevant to M2M systems and sensor networks. The objectives of the ETSI M2M committee include the development and maintenance of an end-to-end architecture for M2M based on internetworking standards. This seems to be a wise choice due to the immediate strengthening of the standardization efforts by including sensor network

	Now	Before 2015	Beyond 2015
Vision	• Connecting objects	• Networked objects	• Intelligent objects
Use	• RFID adoption in logistics and retail • Interoperable frameworks	• Increased interoperability • Industry specific deployments	• Unified network that connects, people and things • Integrated industries
Technology trends	• Smaller and cheaper tages and sensors • Smart multi-band antennas • Higher frequency tags • Miniaturized, embedded readers • Low power chipsets • Reduced energy consumption • Network security • Ad hoc sensor networs • Protocols for distributed processing	• Increasing memory and sensing capacities • Extended range and transmission speed of tag-reader communication • Improved energy management • Better batteries • Interoperability protocols and frequencies • Fault tolerant protocols • Ad hoc hybrid networks • Communication in harsh environments	• Cheaper materials • Executable tags • Intelligent tags • Autonomous tags • New materials • Energy harvesting • Intelligent device coorporation • Global internetworked applications • Self-adaptive systems • Distributed memory and processing
Standards	• RFID security and privacy • Radio frequency usage	• Sector specific standards (IETF, ISO …)	• Interaction standards

Fig. 7. Roadmap for the extrapolation of current technology trends and research topics towards a RFID-enabled Internet of Things. (Adapted from Wiebking et al. (2008)).

integration, naming, addressing, location, QoS, security, charging, management, application, and hardware interfaces for related fields.

As for the Internet Engineering Task Force (IETF) standardiztion activities related to the Internet of Things, it is worth noting that recently the IPv6 over low-power wireless personal area networks (6LoWPAN) IETF group was formed. The 6LoWPAN working group is defining a set of protocols that can be used to integrate sensor nodes into IPv6 networks. Essential protocols composing the 6LoWPAN architecture have already been specified and commercial products that implement the 6LoWPAN protocol stack have been released. Another relevant IETF Working Group is named Routing Over Low power and Lossy networks (ROLL). The working group is currently designing the RPL routing protocol for routing in WSNs – a draft standard which have already got a wide acceptance and a large community support behind it. This will be the basis for routing over low-power and lossy networks including 6LoWPAN. More recently a working group Constrained RESTful Environment (CoRE) formed with the objective to look at the support of RESTful environments for constrained devices such as wireless sensors. This is the key focus of the IETF CoRE working group.

What is also worth pointing out in these standardization areas is the tight collaboration on standards integration as well as the collaboration with other world-wide Interest Groups and Alliances such as IP in Smart Objects (IPSO) Alliance and the ZigBee Alliance. It seems that the whole industry is willing to cooperate on achieving the Internet of Things.

Although there are several standardization efforts to support the integration of heterogeneous networks, a comprehensive framework lack and in a broader perspective for the real-world

integration of all sorts of networked contact-less devices there will be a need for substantial progress in the field.

5.2 Technology trends

In terms of technology evolution the current trends towards smaller, more powerful, and more efficient devices is expected to continue. In WSN, energy consumption is of highest priority and the RF communication design blocks consume the most energy. Wireless sensor network designers strive to reduce the power consumption of the blocks in general.

For the CPU part it is likely that it will approximate the evolution expressed by Moore's law, i.e. doubling of capacity each 18-24 months. The improvement for WSN is likely to be used to reduce size and power consumptions instead of increasing capacity and speed. The use of energy harvesting is an important aspect of RFID/WSN devices. With a combination of energy efficient protocols and energy harvesting methods, the optimal solution for achieving autonomous and long-lasting RFID/WSNs can be reached.

Power management plays a significant role in prolonging node life time. The support of advanced power management schemes needs further research and it needs to be taken from a device-level to a network-level. The IEEE 802.15.4 standard defines only a limited set of power management mechanisms for devices. However, most commercial implementations and industrial standards built on IEEE 802.15.4 seem to deviate from the defined power management mechanisms. Efficient protocol support is also needed for the internetwork based WSN and the ongoing work of the relevant IETF working groups is heading in this direction. This includes protocol optimization for smart devices.

Although movements can have severe impact on the received signal strength a global optimum for the network could still be achieved in some cases. While some protocols already exist that take care of the link layer and networking layer, this area still has a lot of open research issues. More specific link layer protocols need to be developed that take into account the movement of the nodes, in addition to the development of low power features such as an adaptive duty cycle for lowering the idle listening and for adapting to the dynamics of the network. A security framework adapted to internetworked objects in the Internet of Things has to be sufficiently light-weighted to meet the constraints of the RFID/WSN devices. On the other hand it also needs to be capable of providing the in-depth security required for the RFID applications.

5.3 Interoperability

Interoperability issues are also very important because RFID tags increasingly travel across a large number of different geographical and organizational environments, together with the object which they identify, thereby imposing new technical requirements such as multi-protocol, multi-frequency integrated circuits and appropriate antenna solutions for tags. For systems, such as in a supply chain applications, where multiple entities have the ability to access RFID tag related information that is shared across geographic or organizational boundaries, there are issues which need to be addressed through research and development. Not all issues can be addressed by the RFID hardware or middleware or similar technological advancements. They include notably look-up services for efficient data retrieval; business models for data sharing among multiple partners (selective data retrieval, access rights); support for distributed decision-making further than just data sharing; networked RFID systems; interoperability requirements and standards; and network security (access authorization, data encryption, standards).

5.4 Research

The ensuring research targets include the hardware aspects (tags, readers, and embedded systems), the software/system aspects and the networking aspects.

The RFID devices themselves need more capabilities to broaden the range of applications. They need to acquire larger memory, local intelligence, encryption and security features, extended functionalities such as integrated sensors, and much more. To support this functionality, new breakthroughs in battery technology are needed, in particular to enable more energy, less space (or printing of the tag), and more reliability than ever before. Lakafosis et al. (2010) demonstrate prototypes that uses inkjet printed RFIDs integrated with wireless sensors.

Today almost all conventional RFID devices contain a silicon-based microchip. The potential in low cost RFID is split between chip-based technologies and "chip-less" tags. These chip-less tags can still be interrogated through a brick wall and hold data; although more primitive in performance than silicon-based chip tags, they hold the potential of much lower production costs and other advantages that will become clear as the technology matures. Further miniaturization of the tag antenna and more efficient and reliable antenna connecting technologies are seen as another priority before mass introduction is affordable.

Research does not only apply to the RFID tag and/or the reader themselves, but also to the information systems which process the RFID events. Using RFID events within enterprise applications, such as Enterprise Resource Planning (ERP) or Customer Relationship Management (CRM), require new RFID middleware and reorientation of these business applications. Research on RFID software is needed to ensure data security, integrity and quality in large networks. It is also needed to provide solutions enabling a reduction of counterfeit.

The Internet of Things will generate data traffic with patterns that are expected to be significantly different from those observed in the today's Internet. Accordingly, it will also be necessary to define new Quality of Service (QoS) requirements and related support schemes.

6. Related work

Technically the combination of wireless sensor network and RFID gives rise to a number of challenges e.g. for the networking. We need to figure out how to evolve the Internet architecture to handle the novel user scenarios. How can service interoperability be ensured? How can we ensure security and privacy and what are the protocols to use in the system? On top of that, seen from a RFID perspective, we argue that to gain the full potential it is necessary to bring the classic scenario of RFID tags "being connected" to a scenario where we actually have networked RFID objects.

The combination of RFID and wireless sensor networks has been studied in a great range of applications, e.g. from healthcare to transportation/logistics and smart environments (home, office, plant). Mitsugi et al. (2007) argues how medication errors such as outdated treatments orders, inaccurate medical records, and increased costs can be avoided with the use of an integrated RFID sensor network. In the healthcare domain the integration of RFID and wireless sensor networks includes real-time monitoring of temperature, blood pressure measurements, heartbeat rate, heartbeat rate variability and pH value.

Bacheldor (2007) reports that the Ghent University hospital in Belgium has implemented an RFID-based real-time locating system to provide nurses and other caregivers with a patient's location in the event of an emergency. The implemented integrated RFID-sensor network detects when a patient is having cardiac distress and sends to the caregivers an alert indicating

the patient's location. In the proposed prototype Aero Scout T2 active Wi-Fi tags are used, which transmit the tags' unique IDs to the hospitals Wi-Fi network.
Besides a large amount of issues that needs to be address to have a successful internetworking of objects in the Internet of Things with RFID there are also a number of applications that have big potentials for the future. By embedding transponders in everyday object used by individuals, such as books, payment cards, and personal identification we will find new ways to improve our daily lives. As an example, Meingast et al. (2007) discusses the electronic passport that has been investigated in the US.

7. Conclusion

The Internet of Things era represents a gradual evolution from ICT around us to ICT on us. Many challenging issues still need to be addressed and both technological as well as social knots have to be untied before the Internet of Things idea can be widely accepted. The current trend of integrating RFID and WSN seems to be a natural step towards a Internet of Things that provides internetworking opportunities for objects but also allows objects to become smarter and interact more "intelligently" with humans. Generally, it can be concluded that the trend towards an even larger population of connected intelligent objects is irreversible, because the economic value of a system of objects and devices is directly related to the fact that objects are "networked".
Due to the large volume of objects in the Internet of Things cost is a major issue. By introducing RFID technology to internetwork objects a lower system cost compared to wireless sensor network technology can be achieved.
RFID technology is a key enabler for the transition from today's scene of connected objects to the scene of networked objects of the future. For an efficient and smooth transition a number of research issues need to be addressed. In this chapter, we have discussed important aspects of RFID/WSN technology in the Internet of Things with emphasis on what is being done and what are the issues that require further research.

8. References

Atzori, L., Iera, A. & Morabito, G. (2010). The internet of things: A survey, *Computer Networks* 54(15): 2787–2805.
URL: *http://dx.doi.org/10.1016/j.comnet.2010.05.010*

Bacheldor, B. (2007). Belgium hospital combines rfid, sensor to monitor heart patients.
URL: *http://www.rfidjournal.com/article/articleview/ 3120/1/1*

Buckley, J. (2006). *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*, Auerbach Publications 2008. Final report of conference organized by DG information society and media, networks and communication technologies directorate.

Daou, H., Kayssi, A. & Chehab, A. (2008). Rfid security protocols, *Innovations in Information Technology, 2008. IIT 2008. International Conference on*, p. 593.
URL: *http://dx.doi.org/10.1109/INNOVATIONS.2008.4781675*

Floerkemeier, C. & Sarma, S. (2008). An overview of rfid system interfaces and reader protocols, *RFID, 2008 IEEE International Conference on*, p. 232.
URL: *http://dx.doi.org/10.1109/RFID.2008.4519372*

Karl, H. & Willig, A. (2005). *Protocols and Architectures for Wireless Sensor Networks*, John Wiley & Sons.

Khoo, B. (2010). Rfid- from tracking to the internet of things: A review of developments, *Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on Int'l Conference on Cyber, Physical and Social Computing (CPSCom)*, pp. 533–538.
URL: *http://dx.doi.org/10.1109/GreenCom-CPSCom.2010.22*

Krishna, P. & Husalc, D. (2007). Rfid infrastructure, *Communications Magazine, IEEE* 45(9): 4.
URL: *http://dx.doi.org/10.1109/MCOM.2007.4342872*

Lakafosis, V., Rida, A., Vyas, R., Yang, L., Nikolaou, S. & Tentzeris, M. M. (2010). Progress towards the first wireless sensor networks consisting of inkjet-printed, paper-based rfid-enabled sensor tags, *Proceedings of the IEEE* 98(9): 1601.
URL: *http://dx.doi.org/10.1109/JPROC.2010.2049622*

Meingast, M., King, J. & Mulligan, D. K. (2007). Embedded rfid and everyday things: A case study of the security and privacy risks of the u.s. e-passport, *RFID, 2007. IEEE International Conference on*, p. 7.

Mitrokotsa, A. & Douligeris, C. (2010). *Integrated RFID and Sensor Networks: Architectures and Applications*, RFID and Sensor Networks: Architectures, Protocols, Security and Integrations, Auerbach Publications, CRC Press, Taylor and Francis Group, chapter Chapter 18, pp. 511–535.

Mitsugi, J., Inaba, T., Patkai, B., Theodorou, L., Sung, J., Lopez, T. S., Kim, D., McFarlane, D., Hada, H., Kawakita, Y., Osaka, K. & Nakamura, O. (2007). Architecture development for sensor integration in the epcglobal network, *Technical Report WPSWNET-018*, Auto-ID Labs. White paper.
URL: *http://autoidlabs.mit.edu/CS/files/folders/whitepapers/entry3012.aspx*

Papapostolou, A. & Chaouchi, H. (2009). Rfid-assisted movement detection improvement in ip mobility, *Proceedings of the 3rd international conference on New technologies, mobility and security*, NTMS'09, IEEE Press, Piscataway, NJ, USA, pp. 378–382.
URL: *http://dx.doi.org/10.1109/NTMS.2009.5384701*

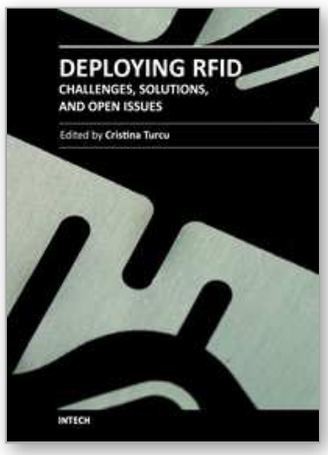
Sharif, A. & Potdar, V. (2008). A critical analysis of rfid security protocols, *Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on*, p. 1357.
URL: *http://dx.doi.org/10.1109/WAINA.2008.212*

Shelby, Z. (2010). Embedded web services, *Wireless Communications, IEEE* 17(6): 52.
URL: *http://dx.doi.org/10.1109/MWC.2010.5675778*

Weis, S., Sarma, S., Rivest, R. & Engels, D. (2004). *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*, Vol. 2802 of *Security in Pervasive Computing*, Springer Berlin / Heidelberg, pp. 50–59.
URL: *http://dx.doi.org/10.1007/978-3-540-39881-3_18*

Wiebking, L., Metz, G., Korpela, M., Nikkanen, M. & Penttilä, K. (2008). A roadmap for rfid applications and technologie, *Technical report*. Final report of the coordination action CE RFID.
URL: *http://www.rfid-in-action.eu/public/results/roadmap*

Zhang, L. & Wang, Z. (2006). Integration of rfid into wireless sensor networks: Architectures, opportunities and challenging problems, *Grid and Cooperative Computing Workshops, 2006. GCCW '06. Fifth International Conference on*, p. 463.
URL: *http://dx.doi.org/10.1109/GCCW.2006.58*



Deploying RFID - Challenges, Solutions, and Open Issues
Edited by Dr. Cristina Turcu

ISBN 978-953-307-380-4
Hard cover, 382 pages
Publisher InTech
Published online 17, August, 2011
Published in print edition August, 2011

Radio frequency identification (RFID) is a technology that is rapidly gaining popularity due to its several benefits in a wide area of applications like inventory tracking, supply chain management, automated manufacturing, healthcare, etc. The benefits of implementing RFID technologies can be seen in terms of efficiency (increased speed in production, reduced shrinkage, lower error rates, improved asset tracking etc.) or effectiveness (services that companies provide to the customers). Leading to considerable operational and strategic benefits, RFID technology continues to bring new levels of intelligence and information, strengthening the experience of all participants in this research domain, and serving as a valuable authentication technology. We hope this book will be useful for engineers, researchers and industry personnel, and provide them with some new ideas to address current and future issues they might be facing.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen